THE GROUPS GENERATED BY TWO OPERATORS SUCH THAT EACH IS TRANSFORMED INTO ITS INVERSE BY THE SQUARE OF THE OTHER

By G. A. Miller

Let s_1, s_2 be any two operators which satisfy the following conditions:

$$s_1^{-2}s_2s_1^2 = s_2^{-1}, \qquad s_2^{-2}s_1s_2^2 = s_1^{-1}.$$

Since s_1^2, s_2^2 transform each other into their inverses, they are either commutative or they generate the quaternion group;* in the former case either both of them are of order two and they generate the four group, or both of them are the identity. The hypothesis that one is of order 2 while the other is the identity leads to an absurdity in view of the given equations. Hence the orders of s_1, s_2 must have one of the following pairs of values: 1, 1; 1, 2; 2, 2; 4, 4; 8, 8. In the first two cases s_1, s_2 would generate the identity and the group of order two respectively. In the third cases they would generate the dihedral group. As these cases are practically trivial, we shall confine our attention in what follows to the groups generated by s_1, s_2 when their common order is either 4 or 8. The main results of this paragraph may be expressed as follows: *If two operators, neither of which is the identity, are such that each is transformed into its inverse by the square of the other, they must have the same order, and this common order is* 2, 4, *or* 8.

We begin with the case when s_1 is of order 8. The quaternion group $\{s_1^2, s_2^2\}$ generated by s_1^2, s_2^2 is invariant under the the group (G) generated by s_1, s_2. This fact results from the following equations:

$$s_1^{-1}s_2^2s_1 = s_1^{-1}s_2^2s_1s_2^{-2}s_2^2 = s_1^{-2}s_2^2, \qquad s_2^{-1}s_1^2s_2 = s_2^{-1}s_1^2s_2s_1^{-2}s_1^2 = s_2^{-2}s_1^2.$$

We shall now prove that the order of s_1s_2 is divisible by 3. This may be

---

* *Quarterly Journal of Mathematics*, vol. 37 (1906), p. 286.

done by means of the following equations:

$$s_1^{-1}s_2^{-1}s_2^2s_2s_1 = s_1^{-2}s_2^2,$$

$$s_1^{-1}s_2^{-1}s_1^{-2}s_2^2s_2s_1 = s_1^{-3}s_1^2s_2^{-1}s_1^{-2}s_2^3s_1 = s_1^{-3}s_2^4s_1 = s_1^{-3}s_1^4s_1 = s_1^2,$$

$$s_1^{-1}s_2^{-1}s_1^2s_2s_1 = s_1^{-1}s_2^{-2}s_1^3 = s_2^{-2}s_2^2s_1^{-1}s_2^{-2}s_1^3 = s_2^{-2}s_1^4 = s_2^2.$$

Since s_2s_1 transforms s_2^2, $s_1^{-2}s_2^2$, s_1^2 cyclically, its order is divisible by three. This proof is equally valid when the order of s_1 is 4, as we made no use of the fact that the order of s_1 was supposed to be 8 except when we stated that $\{s_1^2, s_2^2\}$ was the quaternion group. When s_1 is of order 4 this is the four-group. Hence we have the theorem: *If two operators whose orders exceed* 2 *are such that each is transformed into its inverse by the square of the other, the group generated by them involves operators of order* 3.

The group $\{s_1^2, s_2^2, s_2s_1\}$ is invariant under G, since $\{s_1^2, s_2^2\}$ is invariant under G and the following equations show that s_2s_1 is transformed into an operator of $\{s_1^2, s_2^2, s_2s_1\}$ by s_1 and s_2:

$$s_1^{-1}s_2s_1^2 = s_1^{-1}s_2^{-1}\cdot s_2^2s_1^2, \qquad s_2^{-1}s_2s_1s_2 = s_1s_2 = s_1^2s_1^{-1}s_2^{-1}s_2^2.$$

Hence G contains $\{s_1^2, s_2^2, s_2s_1\}$ as a sub-group of half its order. Since $(s_2s_1)^3$ is invariant under $\{s_1^2, s_2^2, s_2s_1\}$ and s_2s_1 transforms the operators of $\{s_1^2, s_2^2\}$ according to an operator of order 3, it follows that when s_2s_1 is of order 3, that is, when it has its least possible value, $\{s_1^2, s_2^2, s_2s_1\}$ is either the tetrahedral group or the group of order 24 which does not contain a sub-group of order 12, as the order of s_1 is 4 or 8. Hence $\{s_1^2, s_2^2, s_2s_1\}$ has an $(a, 1)$ isomorphism with the tetrahedral group whenever s_2s_1 is of order 3. Since the invariant operators of $\{s_1^2, s_2^2, s_2s_1\}$ are generated by s_1^4 and $(s_2s_1)^3$, it follows that $\{s_1^2, s_2^2, s_2s_1\}$ has an $(a, 1)$ isomorphism with the tetrahedral group regardless of the order of s_2s_1. The quotient group of G with respect to the sub-group generated by s_1^4, $(s_2s_1)^3$ is therefore one of the two groups of order 24 which contain the tetrahedral group. As this quotient group involves operators of order 4, it is the symmetric group of order 24. This proves the fundamental theorem: *If two operators whose orders exceed* 2 *are such that each is transformed into its inverse by the square of the other, they generate a group which has an* $(a, 1)$ *isomorphism with the symmetric group of order* 24. This evidently includes the theorem stated at the end of the preceding paragraph.

From the preceding paragraph it follows that the symmetric group of order 24 is the smallest possible group which may be generated by two operators whose orders exceed 2 and which are such that each is transformed into its inverse by the square of the other. This property may be regarded as a new definition of the symmetric group of order 24. Another definition which results from the preceding equations is this: Two operators of order 4 generate the symmetric group of order 24 provided their product is of order 3 and each of them is transformed into its inverse by the square of the other. Since the operators which correspond to the identity in the given $(a, 1)$ isomorphism between G and the symmetric group of order 24 generate an Abelian group it is clear that G contains exactly 4 Sylow subgroups of order 3^2 and that these are cyclic.

The operators of G which are invariant under $\{s_1^2, s_2^2, s_2s_1\}$ are generated by s_1^4 and $(s_1s_2)^3$, since they are generated by s_1^4 and $(s_2s_1)^3$. We proceed to prove that these operators are transformed into their inverses by the operators of G which are not in $\{s_1^2, s_2^2, s_2s_1\}$. This fact results from the following equations:

$$(s_1^2s_2)^{-1}s_1s_2s_1^{-2}s_1^2s_2 = s_2^{-1}s_1^{-1}s_2^2 = (s_1s_2)^{-1}s_2^2s_1s_2(s_1s_2)^{-1} = s_1^2(s_1s_2)^{-1},$$

$$(s_1s_2s_1^{-2})^3 = s_1s_2s_1^{-2}\cdot s_1s_2s_1^{-2}\cdot s_1s_2s_1^{-2} = (s_1s_2)^2s_2^2s_1s_2s_1^{-2} = (s_1s_2)^3.$$

Since $s_1^2s_2$ transforms $s_1s_2s_1^{-2}$ into its inverse and s_1^4 is invariant under G, the theorem under consideration is proved. Moreover, $(s_1^2s_2)^2 = s_1^2s_2s_1^2s_2 = s_1^4$. That is, G may be obtained by establishing a $(4, m)$ isomorphism between the symmetric group of order 24 and the dihedral group of order $6m$ whenever s_1 is of order 4.

It has been observed that s_1, s_2 may be so chosen that they generate the symmetric group of order 24 and that in all other cases the order of G is a multiple of 24. When s_1, s_2 are of order 4 they may be so selected that the order of G is any arbitrary multiple of 24. To do this we may replace the s_1, s_2 which generates the symmetric group of order 24 by s_1^1, s_2^1, where $s_1^1s_2^1$ are the products of s_1, s_2 respectively into two operators of order two which are independent of s_1, s_2 and whose product is the arbitrary multiple of 3. The same result is obtained by making the symmetric group of order 24 isomorphic with the dihedral group of order $6m$ in such a way that 4 operators of the former correspond to m operators of the latter, where m is arbitrary.

When s_1 is of order 8 the order of G is a multiple of 48, since the order of $\{s_1^2, s_2^2, s_1 s_2\}$ is a multiple of 24 in this case. It has been observed that the latter group is of order 24 and contains no sub-group of order 12 when $s_1 s_2$ is of order 3. When $s_1 s_2$ satisfies this condition G is one of the four groups of order 48 which contain this group of order 24*. As it has a $(2, 1)$ isomorphism with the symmetric group of order 24 and as $s_1^2 s_2$ is of order 4 while s_1 is of order 8, it contains 12 operators of each of the orders 4 and 8 besides those of $\{s_1^2, s_2^2, s_1 s_2\}$. These conditions determine this group of order 48 completely and prove that it is the one known as G_{52}.* *The smallest possible group which is generated by two operators of order* 8 *such that each is transformed into its inverse by the square of the other is the group of order* 48 *known as* G_{52}, and every other group which can be generated by two such operators has an $(\alpha, 1)$ isomorphism with this group. The method used in the preceding paragraph may be employed to show that s_1, s_2 can be so chosen that α has any arbitrary value.

The group of order 48 whose properties were considered in the preceding paragraph may be represented as a substitution group of degree 16 in the following manner:

$$s_1 = ac'eg'bd'fh' \cdot a'de'hb'cf'g, \qquad s_2 = ah'cf'bg'de' \cdot a'gc'eb'hd'f,$$

$$s_1^2 = aebf \cdot cdgh \cdot a'e'b'f' \cdot c'g'd'h', \qquad s_2^2 = acbd \cdot ehfg \cdot a'c'b'd' \cdot e'h'f'g',$$

$$s_2^{-2} s_1 s_2^2 = ah'fd'bg'ec' \cdot a'gf'cb'he'd = s_1^{-1}, \qquad s_1^{-2} s_2 s_1^2 = ae'dg'bf'ch' \cdot a'fd'hb'ec'g = s_2^{-1},$$

$$s_1 s_2 = aed \cdot bfc \cdot a'e'd' \cdot b'f'c'.$$

Since s_1^2, s_2^2 transform each other into their inverses they generate the quaternion group which is transformed into itself by $s_1 s_2$. Hence the remaining substitution of this group of order 48 could easily be written out. When s_1 is of order 4, G is completely determined by the order of $s_1 s_2$ and the fact that each of the operators s_1, s_2 is transformed into its inverse by the square of the other. This is, however, not the case when s_1 is of order 8. In this case it is necessary to specify whether the operator of order 2 generated by $s_1 s_2$ is in $\{s_1^2, s_2^2\}$ or not. For instance, the two substitutions

$$s_1 = ac'eg'bd'fh' \cdot a'de'hb'cf'g, \qquad s_2 = ag'ce'bh'df' \cdot a'hc'fb'gde'$$

are such that each is transformed into its inverse by the square of the other

* *Quarterly Journal of Mathematics*, vol. 30 (1899), p. 258

but their product is of order 6. Since the cube of this product is in $\{s_1^2, s_2^2\}$, they generate the same group of order 48 as the two substitutions given above.

As a rule the most useful groups are those which admit the simplest definitions by means of the laws of combination of their symbols. The groups of genus zero are the most remarkable from this standpoint. The systems whose fundamental properties were considered above appear also to be remarkable from the standpoint of simplicity of definition, and their close contact with the symmetric group of order 24 adds interest. The new definition of the latter group which flows from a study of these systems seems worthy of notice,— not so much on account of its newness as on account of its simplicity. The category of groups considered above suggests the more general question in reference to the groups which are generated by n operators $(n > 2)$ which are such that each is transformed into its inverse by the squares of all the others. While it is known that the squares of these operators would generate either a Hamiltonian group or an Abelian group of order 2^a and of type $(1, 1, 1, \cdots)$* which would be an invariant sub-group and that the order of the group which they generate is divisible by 3 whenever the order of at least one of the generating operators exceeds 2, yet the category of these groups includes so many different types as to make it improbable that much progress can be made along this line. Since every possible symmetric group can be generated by three operators of order 2,† it follows that when $n > 2$ every possible symmetric group could be a quotient group of some groups whose generators would satisfy the given conditions.

UNIVERSITY OF ILLINOIS,
DECEMBER, 1906.

---

* *Quarterly Journal of Mathematics*, vol. 37 (1906), p. 286.

† Cf. *Bulletin of the American Mathematical Society*, vol. 7 (1901), p. 426.